

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-249286

(43) 公開日 平成8年(1996)9月27日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0	9364-5L	G 0 6 F 15/00	3 3 0 Z
G 0 7 B 1/00			G 0 7 B 1/00	A
G 0 9 C 1/00		7259-5J	G 0 9 C 1/00	
H 0 4 L 9/06			H 0 4 L 9/02	Z
9/14				

審査請求 未請求 請求項の数17 O L (全 15 頁)

(21) 出願番号 特願平7-54069

(22) 出願日 平成7年(1995)3月14日

(71) 出願人 000002945

オムロン株式会社

京都府京都市右京区花園土堂町10番地

(72) 発明者 出水 法俊

京都府京都市右京区花園土堂町10番地 オ

ムロン株式会社内

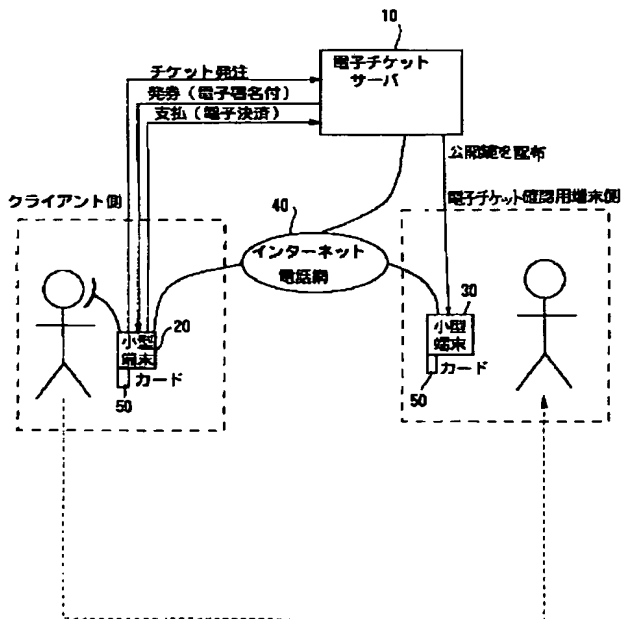
(74) 代理人 弁理士 和田 成則

(54) 【発明の名称】 電子データ送受信システム

(57) 【要約】

【目的】 送信された電子データの不正利用を防止するとともに、データ送信の秘密の保持性に優れた電子データ送受信システムを提供する。

【構成】 サーバ端末(10)は、クライアント端末(20)からの送信要求に対応して暗号化した通し番号を付与した電子データをクライアント端末(20)に送信するとともに、送信した電子データを記憶し、また、クライアント端末(20)は、サーバ端末(10)から送信された電子データを受信してカード50に書き込むことにより電子データの受信を行い、また、チェック端末(30)は、カード(50)に書き込まれた電子データとサーバ端末(10)に記憶した電子データとを照合することにより電子データの確認を行う。



1

【特許請求の範囲】

【請求項 1】 電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、

上記サーバは、

上記クライアントからの送信要求に対応して暗号化した通し番号を付与した電子データを上記クライアントに送信する電子データ送信手段と、

上記電子データ送信手段で送信した電子データを記憶する電子データ記憶手段とを具備し、

上記クライアントは、

上記電子データ送信手段により上記サーバから送信された電子データを受信することにより上記電子データの受信を行う電子データ受信手段を具備し、

上記電子データ確認端末は、

上記電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより上記電子データの確認を行う電子データ確認手段を具備することを特徴とする電子データ送受信システム。

【請求項 2】 上記電子データ送信手段は、

上記クライアントからの送信要求に対応して電子データを生成する電子データ生成手段と、

上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、

上記通し番号付与手段で暗号化した通し番号が付与された電子データを上記クライアントに送信する送信手段と、

を具備することを特徴とする請求項 1 記載の電子データ送受信システム。

【請求項 3】 上記クライアントは、

上記電子データを書き込み可能なカードを有し、

上記電子データ送信手段により上記サーバから送信された電子データを受信して上記カードに書き込むことにより上記電子データを受信することを特徴とする請求項 1 記載の電子データ送受信システム。

【請求項 4】 上記電子データ確認端末は、

上記クライアントで受信した電子データの電子データに付与された暗号化した通し番号を解読することにより上記電子データの確認を行うことを特徴とする請求項 1 記載の電子データ送受信システム。

【請求項 5】 上記電子データ送信手段は、

上記クライアントからの送信要求に対応して電子データを生成する電子データ生成手段と、

上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、

上記通し番号付与手段で暗号化した通し番号が付与された電子データの全体を暗号化する暗号化手段と、

2

上記暗号化手段で暗号化した電子データを上記クライアントに送信する送信手段と、
を具備することを特徴とする請求項 1 記載の電子データ送受信システム。

【請求項 6】 上記クライアントは、

上記暗号化手段で暗号化された電子データを解読する解読手段を具備することを特徴とする請求項 5 記載の電子データ送受信システム。

【請求項 7】 電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、

上記クライアントは、

上記サーバに対して上記クライアント側で作成した暗号キーワードを含む電子データの送信を要求する送信要求手段を具備し、

上記サーバは、

上記クライアントからの送信要求に対応して上記暗号キーワードを含む電子データを上記クライアントに送信する電子データ送信手段と、

上記電子データ送信手段で送信した電子データを記憶する電子データ記憶手段とを具備し、

上記クライアントは、

上記電子データ送信手段により上記サーバから送信された電子データを受信する電子データ受信手段を具備し、

上記電子データ確認端末は、

上記電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより上記電子データの確認を行う電子データ確認手段を具備することを特徴とする電子データ送受信システム。

【請求項 8】 上記送信要求手段は、

上記クライアント側で作成した暗号キーワードを含む電子データの送信要求の全体を暗号化して上記サーバに対して送信することを特徴とする請求項 7 記載の電子データ送受信システム。

【請求項 9】 上記電子データ送信手段は、

上記暗号キーワードを含む電子データの全体を暗号化して上記サーバに対して送信することを特徴とする請求項 7 記載の電子データ送受信システム。

【請求項 10】 上記クライアントは、

上記暗号化手段で暗号化された電子データを解読する解読手段を具備することを特徴とする請求項 9 記載の電子データ送受信システム。

【請求項 11】 電子データを送信するサーバと該サーバと回線を介して接続され該サーバから送信された電子データを受信するクライアントとを具備する電子データ送受信システムにおいて、

上記クライアントは、

3

上記電子データの送信要求を生成する送信要求生成手段と、
 上記送信要求生成手段で発生された送信要求を上記クライアントの秘密鍵を用いて暗号化する第1の暗号化手段と、
 上記第1の暗号化手段に暗号化された送信要求を上記サーバの公開鍵を用いて暗号化する第2の暗号化手段と、
 上記第2の暗号化手段で暗号化された送信要求を上記サーバに送信する送信要求手段と、
 を具備することを特徴とする電子データ送受信システム。

【請求項12】 上記サーバは、
 上記送信要求手段により送信された送信要求を受信する送信要求受信手段と、
 上記送信要求受信手段で受信した送信要求を上記サーバの秘密鍵を用いて復号化する第1の復号化手段と、
 上記第1の復号化手段で復号化された送信要求を上記クライアントの公開鍵を用いて復号化することにより上記送信要求の適否の照合を行う第1の照合手段と、
 上記第1の照合手段により上記送信要求が適正であると判定された場合は、上記送信要求に対応する電子データを生成する電子データ生成手段と、
 上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、
 上記通し番号付与手段で暗号化した通し番号が付与された電子データを上記サーバの秘密鍵を用いて暗号化する第3の暗号化手段と、
 上記第3の暗号化手段で暗号化された電子データを上記クライアントの公開鍵を用いて暗号化する第4の暗号化手段と、
 上記第4の暗号化手段で暗号化された電子データを上記サーバに送信する電子データ送信手段と、
 を具備することを特徴とする請求項1記載の電子データ送受信システム。

【請求項13】 上記クライアントは、
 上記電子データ送信手段から送信された電子データを受信する電子データ受信手段と、
 上記電子データ受信手段で受信した電子データを上記クライアントの秘密鍵を用いて復号化する第2の復号化手段と、
 上記第2の復号化手段で復号化された電子データを上記サーバの公開鍵を用いて復号化することにより上記電子データの適否の照合を行う第2の照合手段と、
 上記第2の照合手段で上記電子データが適正であると判定された場合は、上記電子データを記録する記録手段と、
 を具備することを特徴とする請求項1記載の電子データ送受信システム。

【請求項14】 電子データを送信するサーバと該サーバと回線を介して接続され該サーバから送信された電子

4

データを受信するクライアントとを具備する電子データ送信システムにおいて、
 上記クライアントは、
 上記電子データの送信要求を生成する送信要求生成手段と、
 上記送信要求生成手段で発生された送信要求に乱数を付与する乱数付与手段と、
 上記乱数付与手段で乱数が付与された送信要求を上記クライアントの秘密鍵を用いて暗号化する第1の暗号化手段と、
 上記第1の暗号化手段で暗号化された送信要求を上記サーバの公開鍵を用いて暗号化する第2の暗号化手段と、
 上記第2の暗号化手段で暗号化された送信要求を上記サーバに送信する送信要求手段と、
 を具備することを特徴とする電子データ送受信システム。

【請求項15】 上記サーバは、
 上記送信要求手段により送信された送信要求を受信する送信要求受信手段と、
 上記送信要求受信手段で受信した送信要求を上記サーバの秘密鍵を用いて復号化する第1の復号化手段と、
 上記第1の復号化手段で復号化された送信要求を上記クライアントの公開鍵を用いて復号化することにより上記送信要求の適否の照合を行う第1の照合手段と、
 上記第1の照合手段により上記送信要求が適正であると判定された場合は、上記送信要求に対応する電子データを生成する電子データ生成手段と、
 上記電子データ生成手段で生成された電子データを上記サーバの秘密鍵を用いて暗号化する第3の暗号化手段と、
 上記第3の暗号化手段で暗号化された電子データを上記クライアントの公開鍵を用いて暗号化する第4の暗号化手段と、
 上記第4の暗号化手段で暗号化された電子データを上記サーバに送信する電子データ送信手段と、
 を具備することを特徴とする請求項14記載の電子データ送受信システム。

【請求項16】 上記クライアントは、
 上記電子データ送信手段から送信された電子データを受信する電子データ受信手段と、
 上記電子データ受信手段で受信した電子データを上記クライアントの秘密鍵を用いて復号化する第2の復号化手段と、
 上記第2の復号化手段で復号化された電子データを上記サーバの公開鍵を用いて復号化することにより上記電子データの適否の照合を行う第2の照合手段と、
 上記第2の照合手段で上記電子データが適正であると判定された場合は、上記電子データを記録する記録手段と、
 を具備することを特徴とする請求項14記載の電子データ

10

20

30

40

50

タ送受信システム。

【請求項 17】 電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、
上記クライアントは、
上記サーバから送信された電子データに対応する上記サーバの秘密鍵を用いて暗号化された電子データを記憶する記憶手段と、
上記記憶手段に記憶された上記電子データを取り出す取出手段と、
上記取出手段により取出された電子データを上記電子データ確認端末の公開鍵を用いて暗号化する暗号化手段と、
上記暗号化手段で暗号化されたデータを上記電子データ確認端末に送信する送信手段と、
を具備し、
上記電子データ確認端末は、
上記送信手段により送信された電子データを受信する受信手段と、
上記受信手段で受信した電子データを上記電子データ確認端末の秘密鍵を用いて復号化する復号化手段と、
上記復号化手段で復号化した電子データの適否を確認する確認手段と、
を具備することを特徴とする電子データ送受信システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 この発明は電子データ送受信システムに関し、特に送信された電子データの不正利用を防止するように改良した電子データ送受信システムに関する。

【0002】

【従来の技術】 最近、S-RAMやEEPROM等の半導体メモリを内蔵したICカードを用いることにより、ホテルの利用チケット、電車、飛行機、船のチケット、映画館、コンサートのチケットなどをインターネット電話網を介して電子的に発券する電子チケット発券システムが考えられている。この電子チケット発券システムとしては、従来、特開平6-236464号公報に開示されたものが知られている。

【0003】 ところで、この種の電子チケット発券システムは、一般には、電子チケットを発券するサーバと該サーバから発券された電子チケットを受券するクライアントと該クライアントで受券した電子チケットの確認を行う電子チケット確認端末とを具備して構成されるが、ここで、サーバから発券されるチケットが秘密性を有するものもあり、また、サーバから発券したチケットのクライアント側による不正利用を如何にして防止するかが

重大な問題である。

【0004】

【発明が解決しようとする課題】 しかしながら、従来の特開平6-236464号公報に開示された電子チケット発券システム等においては、チケット発券に対する秘密の保持性および不正利用の防止の点において問題がある。

【0005】 そこで、この発明は、送信された電子チケットの不正利用を防止するとともに、チケット発券の秘密の保持性に優れたシステムを提供することを目的とする。

【0006】

【課題を解決するための手段】 上記目的を達成するため、この発明は、電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、上記サーバは、上記クライアントからの送信要求に対応して暗号化した通し番号を付与した電子データを上記クライアントに送信する電子データ送信手段と、上記電子データ送信手段で送信した電子データを記憶する電子データ記憶手段とを具備し、上記クライアントは、上記電子データ送信手段により上記サーバから送信された電子データを受信することにより上記電子データの受信を行う電子データ受信手段を具備し、上記電子データ確認端末は、上記電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより上記電子データの確認を行う電子データ確認手段を具備することを特徴とする。

【0007】 また、この発明は、電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、上記クライアントは、上記サーバに対して上記クライアント側で作成した暗号キーワードを含む電子データの送信を要求する送信要求手段を具備し、上記サーバは、上記クライアントからの送信要求に対応して上記暗号キーワードを含む電子データを上記クライアントに送信する電子データ送信手段と、上記電子データ送信手段で送信した電子データを記憶する電子データ記憶手段とを具備し、上記クライアントは、上記電子データ送信手段により上記サーバから送信された電子データを受信する電子データ受信手段を具備し、上記電子データ確認端末は、上記電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより上記電子データの確認を行う電子データ確認手段を具備することを特徴とする。

【0008】 また、この発明は、電子データを送信するサーバと該サーバと回線を介して接続され該サーバから

7

送信された電子データを受信するクライアントとを具備する電子データ送受信システムにおいて、上記クライアントは、上記電子データの送信要求を生成する送信要求生成手段と、上記送信要求生成手段で発生された送信要求を上記クライアントの秘密鍵を用いて暗号化する第1の暗号化手段と、上記第1の暗号化手段で暗号化された送信要求を上記サーバの公開鍵を用いて暗号化する第2の暗号化手段と、上記第2の暗号化手段で暗号化された送信要求を上記サーバに送信する送信要求手段と、を具備することを特徴とする。

【0009】また、この発明は、電子データを送信するサーバと該サーバと回線を介して接続され該サーバから送信された電子データを受信するクライアントとを具備する電子データ送受信システムにおいて、上記クライアントは、上記電子データの送信要求を生成する送信要求生成手段と、上記送信要求生成手段で発生された送信要求に乱数を付与する乱数付与手段と、上記乱数付与手段で乱数が付与された送信要求を上記クライアントの秘密鍵を用いて暗号化する第1の暗号化手段と、上記第1の暗号化手段で暗号化された送信要求を上記サーバの公開鍵を用いて暗号化する第2の暗号化手段と、上記第2の暗号化手段で暗号化された送信要求を上記サーバに送信する送信要求手段と、を具備することを特徴とする。

【0010】また、この発明は、電子データを送信するサーバと該サーバから送信された電子データを受信するクライアントと該クライアントで受信した電子データの確認を行う電子データ確認端末とを具備する電子データ送受信システムにおいて、上記クライアントは、上記サーバから送信された電子データに対応する上記サーバの秘密鍵を用いて暗号化された電子データを記憶する記憶手段と、上記記憶手段に記憶された上記電子データを取り出す取出手段と、上記取出手段により取出された電子データを上記電子データ確認端末の公開鍵を用いて暗号化する暗号化手段と、上記暗号化手段で暗号化されたデータを上記電子データ確認端末に送信する送信手段と、を具備し、上記電子データ確認端末は、上記送信手段により送信された電子データを受信する受信手段と、上記受信手段で受信した電子データを上記電子データ確認端末の秘密鍵を用いて復号化する復号化手段と、上記復号化手段で復号化した電子データの適否を確認する確認手段と、を具備することを特徴とする。

【0011】

【作用】この発明の電子データ送受信システムにおいて、サーバは、電子データ送信手段により、クライアントからの送信要求に対応して暗号化した通し番号を付与した電子データをクライアントに送信するとともに、電子データ記憶手段により、電子データ送信手段で送信した電子データを記憶する。また、クライアントは、電子データ受信手段により、電子データ送信手段によりサー

8

バから送信された電子データを受信することにより電子データの受信を行う。また、電子データ確認端末は、電子データ確認手段により、電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより電子データの確認を行う。

【0012】ここで、上記電子データ送信手段は、上記クライアントからの送信要求に対応して電子データを生成する電子データ生成手段と、上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、上記通し番号付与手段で暗号化した通し番号が付与された電子データを上記クライアントに送信する送信手段と、を具備して構成することができる。

【0013】また、上記クライアントは、上記電子データを書き込み可能なカードを有し、上記電子データ送信手段により上記サーバから送信された電子データを受信して上記カードに書き込むことにより上記電子データを受信するように構成することができる。

【0014】また、上記電子データ確認端末は、上記クライアントで受信した電子データの電子データに付与された暗号化した通し番号を解読することにより上記電子データの確認を行うように構成することができる。

【0015】また、上記電子データ送信手段は、上記クライアントからの送信要求に対応して電子データを生成する電子データ生成手段と、上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、上記通し番号付与手段で暗号化した通し番号が付与された電子データの全体を暗号化する暗号化手段と、上記暗号化手段で暗号化した電子データを上記クライアントに送信する送信手段と、を具備して構成することができる。

【0016】また、上記クライアントは、上記暗号化手段で暗号化された電子データを解読する解読手段を具備することにより、受信した電子データを確認できるように構成することもできる。

【0017】また、この発明の電子データ送受信システムにおいて、クライアントは、送信要求手段により、サーバに対してクライアント側で作成した暗号キーワードを含む電子データの送信要求を送信し、サーバは、電子データ送信手段により、クライアントからの送信要求に対応して暗号キーワードを含む電子データをクライアントに送信するとともに、電子データ記憶手段により、電子データ送信手段で送信した電子データを記憶する。また、クライアントは、電子データ受信手段により、電子データ送信手段によりサーバから送信された電子データを受信することにより電子データの受信を行う。また、電子データ確認端末は、電子データ確認手段により、電子データ受信手段で受信した電子データと電子データ記憶手段に記憶した電子データとを照合することにより電

子データの確認を行う。

【0018】ここで、上記送信要求手段は、上記クライアント側で作成した暗号キーワードを含む電子データの送信要求の全体を暗号化して上記サーバに対して送信するように構成することができる。

【0019】また、上記電子データ送信手段は、上記暗号キーワードを含む電子データの全体を暗号化して上記サーバに対して送信するように構成することができる。

【0020】また、上記クライアントは、上記暗号化手段で暗号化された電子データを解読する解読手段を具備することにより、受信した電子データを確認できるように構成することもできる。

【0021】また、この発明の電子データ送受信システムにおいて、クライアントは、送信要求生成手段により、電子データの送信要求を生成し、第1の暗号化手段により、送信要求生成手段で発生された送信要求をクライアントの秘密鍵を用いて暗号化し、第2の暗号化手段により、第1の暗号化手段で暗号化された送信要求をサーバの公開鍵を用いて更に暗号化し、送信要求手段により、第2の暗号化手段で暗号化された送信要求をサーバに送信する。

【0022】ここで、上記サーバは、上記送信要求手段により送信された送信要求を受信する送信要求受信手段と、上記送信要求受信手段で受信した送信要求を上記サーバの秘密鍵を用いて復号化する第1の復号化手段と、上記第1の復号化手段で復号化された送信要求を上記クライアントの公開鍵を用いて復号化することにより上記送信要求の適否の照合を行う第1の照合手段と、上記第1の照合手段により上記送信要求が適正であると判定された場合は、上記送信要求に対応する電子データを生成する電子データ生成手段と、上記電子データ生成手段で生成された電子データに暗号化した通し番号を付与する通し番号付与手段と、上記通し番号付与手段で暗号化した通し番号が付与された電子データを上記サーバの秘密鍵を用いて暗号化する第3の暗号化手段と、上記第3の暗号化手段で暗号化された電子データを上記クライアントの公開鍵を用いて暗号化する第4の暗号化手段と、上記第4の暗号化手段で暗号化された電子データを上記サーバに送信する電子データ送信手段と、を具備して構成することができる。

【0023】また、上記クライアントは、上記電子データ送信手段から送信された電子データを受信する電子データ受信手段と、上記電子データ受信手段で受信した電子データを上記クライアントの秘密鍵を用いて復号化する第2の復号化手段と、上記第2の復号化手段で復号化された電子データを上記サーバの公開鍵を用いて復号化することにより上記電子データの適否の照合を行う第2の照合手段と、上記第2の照合手段で上記電子データが適正であると判定された場合は、上記電子データを記録する記録手段と、を具備して構成することができる。

【0024】また、この発明の電子データ送受信システムにおいて、クライアントは、送信要求生成手段により、電子データの送信要求を生成し、乱数付与手段により、送信要求生成手段で発生された送信要求に乱数を付与し、第1の暗号化手段により、乱数付与手段で乱数が付与された送信要求をクライアントの秘密鍵を用いて暗号化し、第2の暗号化手段により、第1の暗号化手段で暗号化された送信要求をサーバの公開鍵を用いて更に暗号化し、送信要求手段により、第2の暗号化手段で暗号化された送信要求をサーバに送信する。

【0025】ここで、上記サーバは、上記送信要求手段により送信された送信要求を受信する送信要求受信手段と、上記送信要求受信手段で受信した送信要求を上記サーバの秘密鍵を用いて復号化する第1の復号化手段と、上記第1の復号化手段で復号化された送信要求を上記クライアントの公開鍵を用いて復号化することにより上記送信要求の適否の照合を行う第1の照合手段と、上記第1の照合手段により上記送信要求が適正であると判定された場合は、上記送信要求に対応する電子データを生成する電子データ生成手段と、上記電子データ生成手段で生成された電子データを上記サーバの秘密鍵を用いて暗号化する第3の暗号化手段と、上記第3の暗号化手段で暗号化された電子データを上記クライアントの公開鍵を用いて暗号化する第4の暗号化手段と、上記第4の暗号化手段で暗号化された電子データを上記サーバに送信する電子データ送信手段と、を具備して構成することができる。

【0026】また、上記クライアントは、上記電子データ送信手段から送信された電子データを受信する電子データ受信手段と、上記電子データ受信手段で受信した電子データを上記クライアントの秘密鍵を用いて復号化する第2の復号化手段と、上記第2の復号化手段で復号化された電子データを上記サーバの公開鍵を用いて復号化することにより上記電子データの適否の照合を行う第2の照合手段と、上記第2の照合手段で上記電子データが適正であると判定された場合は、上記電子データを記録する記録手段と、を具備して構成することができる。

【0027】また、この発明の電子データ送信システムにおいて、クライアントは、記憶手段により、サーバから送信された電子データに対応するサーバの秘密鍵を用いて暗号化された電子データを記憶し、取出手段により、記憶手段に記憶された電子データを取り出し、暗号化手段により、取出手段により取出された電子データを電子データ確認端末の公開鍵を用いて暗号化し、送信手段により、暗号化手段で暗号化されたデータを電子データ確認端末に送信する。また、電子データ確認端末は、受信手段により、送信手段により送信された電子データを受信し、復号化手段により、受信手段で受信した電子データを電子データ確認端末の秘密鍵を用いて復号化し、確認手段により、復号化手段で復号化した電子デー

タの適否を確認する。

【0028】

【実施例】以下、この発明に係わる電子データ送受信システムの実施例を添付図面に基づいて詳細に説明する。

【0029】図1は、この発明に係わる電子データ送受信システムの一実施例の概略構成を示すブロック図である。

【0030】図1において、この電子データ送受信システムは、電子データを送信する電子データサーバ10を中心に、電子データサーバ（以下、サーバ端末という）10から送信された電子データを受信するクライアント側に設けられた小型端末（以下、クライアント端末という）20およびクライアント側で受信した電子データの利用時に該電子データの確認を行う電子データ確認用端末側に設けられた小型端末（以下チェック端末という）30を具備して構成される。

【0031】ここで、クライアント端末20およびチェック端末30は、インターネット電話網40を介してサーバ端末10に接続されている。

【0032】なお、図1においては、クライアント端末20およびチェック端末30をそれぞれ1台ずつ示したが、実際の構成において、クライアント端末20は一般の家庭または会社に配設されるもので、このクライアント端末20は多数配設されており、また、チェック端末30は、この電子データの利用箇所、例えば、ホテル、駅、コンサート会場などにそれぞれ配設されるもので、このチェック端末30も多数配設されている。

【0033】また、クライアント端末20は、S-RAMやEEP-ROM等の半導体メモリを内蔵したICカード等からなるデータ書き込み／読み出し可能な電子データカード（以下、カードという）50に対してデータを書き込み／読み出しすることができるカードライタ／リーダを有しており、このカード50に対してサーバ端末10から送信された電子データの対応する電子データを書き込むことにより電子データを受信するチケット受信処理を行う。

【0034】また、チェック端末30は、クライアント端末20によりチケット受信処理されたカード50からデータを読み出し／書き込みすることのできるカードリーダー／ライタを有しており、このカード50から所望の電子データを読み出すことにより、この電子データが適正であるか否かのチェックを行う。

【0035】サーバ端末10は、クライアント側からの送信要求によりクライアント端末20を介して電子データを送信する。ここで、この実施例において、電子データの内容としては、

- 1) ホテル等の利用チケット
- 2) 電車、飛行機、船等のチケット
- 3) 映画館、コンサート等のチケット
- 3) 競馬、競輪等のチケット

等を想定している。

【0036】また、クライアント側からの送信要求としては、

- 1) 電話回線を用いた電話による音声通信で行われる送信要求
- 2) 電話回線を用いたファクシミリによる画像通信で行われる送信要求
- 3) 電話回線を用いたパーソナルコンピュータ、ファミリーコンピュータからのデータ通信で行われる送信要求
- 4) 電子データを送信する店頭における口答による送信要求
- 5) クライアント端末20からのインターネット電話網40を用いた送信要求等が考えられる。

【0037】いずれの送信要求を採用しても、サーバ端末10は、この送信要求によりクライアント端末20を介して電子データを送信する。

【0038】なお、4)の電子データを送信する店頭における口答による送信要求を採用する場合は、クライアント端末20は、この電子データを送信する店頭に配設されることになる。

【0039】なお、以下の説明においては、クライアント側では、5)のクライアント端末20からのインターネット電話網40を用いた送信要求を行うものとして各部の動作説明を行う。

【0040】サーバ端末10は、クライアント側のクライアント端末20からの送信要求（チケットの発注）をインターネット電話網40を介して受信すると、この送信要求に対応する所定の電子データを送信する電子データ送信処理を実行する。ここで、この電子データ送信処理は、サーバ端末10からインターネット電話網40を介してクライアント側のクライアント端末20に送信要求に対応する電子データを送信するとともに、この送信した電子データをサーバ端末10側に格納することにより行われる。ここで、サーバ端末10からクライアント端末20に送信される電子データには、後に詳述するように、クライアント側を特定するための電子署名が付される。

【0041】また、クライアント側のクライアント端末20は、このサーバ端末10からの電子データを受信して、この受信した電子データをカード50に書き込むことにより電子データの受信処理を行う。

【0042】また、クライアント側のクライアント端末20は、このサーバ端末10からの電子データの受信処理を行った後、この電子データの代金を電子決済により支払うことができる。

【0043】ところで、この実施例においては、サーバ端末10による電子データ送信処理において、クライアント側で受信した電子データのクライアント側での不正利用を防止するために、サーバ端末10からクライアント側のクライアント端末20に送信する電子データに、

1) 暗号化された通し番号を付与する
 2) 発呼要求の際にクライアント側から送信された暗号キーワードを付与する処理を行い、この電子データを使用する際には、チェッカ端末30で暗号化された通し番号または暗号キーワードのチェックを行うように構成される。

【0044】ここで、1)の処理を採用した場合は、通し番号が暗号化されているため、この通し番号をクライアント側では解読することができないため、この通し番号の改竄により同一の電子データを繰り返し何回も使用するという不正利用を防止することができ、また、2)の処理を採用した場合は、この電子データの使用時に暗号キーワードが必要となるため、この電子データの第三者による不正利用を防止することができる。

【0045】また、この実施例においては、サーバ端末10からクライアント側のクライアント端末20へ電子データを送信するに際して、この送信データ全てを暗号化してクライアント端末20へ送信するように構成される。

【0046】このような構成によると、サーバ端末10からクライアント端末20への電子データの送信途中において、この電子データを第三者に盗聴されたとしても、この第三者によってはこの電子データを解読することはできないので、電子データ送信の秘密性が保持される。この構成は、インターネット電話網40として、不特定多数がアクセス可能な網を用いる場合等に特に有効である。

【0047】なお、サーバ端末10からクライアント端末20へ送信される電子データを暗号化する構成において、クライアント側でこの暗号化した電子データを解読することができるように構成すれば、クライアント側で受信した電子データの内容の確認を行うことができる。なお、クライアント側で暗号化した電子データを解読することができるように構成した場合で、電子データに暗号化された通し番号を付与する構成をとった場合も、この暗号化された通し番号はクライアント側では解読することができないようにすれば、クライアント側により通し番号を改竄して同一の電子データを繰り返し何回も使用するという不正重複利用を防止することができる。

【0048】また、チェッカ端末30は、この電子データの利用箇所において、利用電子データが適正であるか否かのチェックを行う。具体的には、クライアント側での電子データの受信は、上述したように、サーバ端末10から送信された電子データをカード50に書き込むことにより行われるので、この受信した電子データを利用する場合は、この電子データが書き込まれたカード50をこの電子データの利用箇所まで利用者が携帯して行き、このカード50をこの電子データの利用箇所に配設されたチェッカ端末30に挿入することにより、この電子データのチェックが行われる。

【0049】このチェックにおいて、この電子データが適正なものであるとすると、この電子データの利用が可能になる。例えば、この電子データがホテル等の利用チケットの場合は、このホテルの利用が可能になり、電車、飛行機、船等のチケットの場合は、電車、飛行機、船等の利用が可能になり、映画館、コンサート等のチケットの場合は映画館、コンサート等の入場が可能になり、競馬、競輪等のチケットの場合は、馬券、車券等の購入が可能になる。

10 【0050】このチェッカ端末30には、サーバ端末10から後に詳述する公開鍵および送信したチェックデータが配布されており、チェッカ端末30では、この公開鍵を用いてカード50に書き込まれた電子データを解読し、その結果この電子データが適正であるか否かのチェックを行う。

【0051】図2は、サーバ端末10の具体的構成をブロック図で示したものである。図2において、このサーバ端末10は、基本ブロック100と送信した電子データ等を格納するデータベース12を具備して構成される。

20 【0052】ここで、基本ブロック100は、図3に示しように、識別子発生装置101、時計102、電源103、通信部104、作業域105、暗号処理装置110を具備して構成され、暗号処理装置110は、電子署名装置111、電子署名参照装置112、暗号化装置113、復号化装置114、鍵管理装置120を具備し、鍵管理装置120は、公開鍵管理装置121、秘密鍵管理装置122を具備している。

30 【0053】ここで、識別子発生装置101はこの基本ブロック100が搭載された機器の識別子を発生するもの、時計102は時刻を計時するもので、電子データの送信時刻等を管理するもの、電源103はこの基本ブロック100が搭載された機器の駆動電源を与えるもので、商用電源からの供給を受けるものまたは電池から構成されるもの、通信部104はこの基本ブロック100が搭載された機器と他の機器との間の通信を行うもの、作業域105は、この基本ブロック100が搭載された機器の各種データ処理を行う箇所、暗号処理装置110はこの基本ブロック100が搭載された機器における各種暗号処理を行うものである。

40 【0054】また、電子署名装置111は後に詳述する電子署名処理を行うもの、電子署名参照装置112は後に詳述する電子署名参照処理を行うもの、暗号化装置113はデータの暗号化処理を行うもの、復号化装置114は暗号化されたデータの復号化処理を行うもの、鍵管理装置120は、電子署名装置111による電子署名処理、電子署名参照装置112による電子署名参照処理、暗号化装置113による暗号化処理、復号化装置114による復号化処理で用いる公開鍵および秘密鍵を管理するものである。

【0055】また、公開鍵管理装置121は上記公開鍵を管理するもの、秘密鍵管理装置122は上記秘密鍵を管理するものである。なお、このこの公開鍵および秘密鍵については後に詳述する。

【0056】図4は、クライアント端末20の具体的構成をブロック図で示したものである。図4において、このクライアント端末20は、基本ブロック100、入力装置21、記憶域22、表示装置23、記録装置24、電子決済装置25を具備して構成される。

【0057】ここで、基本ブロック100は図3に詳述したものと同じのものである。

【0058】また、入力装置21はこのクライアント端末20を動作させるための各種データおよびコマンドを入力するもの、記憶域22はこのクライアント端末20の処理のための作業域を構成するもの、表示装置23はこのクライアント端末20の動作状態等を含む各種情報を表示するもの、記録装置24は、例えばサーバ端末10から受信した電子データ等を記録するもの、電子決済装置25は電子データを受信した際の代金を電子決済するものである。

【0059】図5は、チェッカ端末30の具体的構成をブロック図で示したものである。図5において、このチェッカ端末30は、基本ブロック100、確認装置31、表示装置32を具備して構成される。

【0060】ここで、基本ブロック100は図3に詳述したものと同じのものである。

【0061】また、確認装置31は利用電子データが適正か否かを確認するもの、表示装置32は確認装置31による確認結果等を表示するものである。

【0062】図6は、図1に示した電子データ送信システムにおける電子データ予約手順の具体例を示したもので、この図6の示すものにおいては、暗号化した通し番号を用いた場合におけるクライアント側のクライアント端末20およびサーバ側のサーバ端末10の動作を示している。

【0063】ところで、この実施例においてはクライアント側およびサーバ側における電子署名および暗号化／復号化処理のために、クライアント側のクライアント端末20は、秘密鍵Kcsおよび公開鍵Kcpを有しており、また、サーバ側のサーバ端末10は、秘密鍵Kssおよび公開鍵Kspを有している。

【0064】ここで、秘密鍵Kcsは、クライアント側における電子署名に用いるもので、この秘密鍵Kcsで暗号化されたデータは、対応する公開鍵Kcpを用いることにより、サーバ側で復号化することができる。

【0065】また、公開鍵Kspは、クライアント側における暗号化に用いるもので、公開鍵Kspで暗号化されたデータは、対応する秘密鍵Kssを用いないと復号化できない。

【0066】また、秘密鍵Kssはサーバ側における電

子署名に用いるもので、この秘密鍵Kssで暗号化されたデータは、対応する公開鍵Kspを用いることにより、クライアント側で復号化することができる。

【0067】また、公開鍵Kcpは、サーバ側における暗号化に用いるもので、公開鍵Kcpで暗号化されたデータは、対応する秘密鍵Kcsを用いないと復号化できない。

【0068】図6において、クライアント側からサーバ側に対して送信要求をする場合は、まず、この送信要求に対応するリクエストRを生成する（ステップ201）。そして、このリクエストRをクライアントの秘密鍵Kcsで暗号化することにより電子署名を行う（ステップ202）。

【0069】次に、この電子署名を行ったリクエストR（Kcs）を更にサーバの公開鍵Kspで暗号化し（ステップ203）、この暗号化したリクエストR（Kcs、Ksp）をサーバ側に送信する（ステップ204）。

【0070】サーバ側では、このリクエストR（Kcs、Ksp）を受信し（ステップ205）、この受信したリクエストR（Kcs、Ksp）をサーバの秘密鍵Kssで復号化する（ステップ206）。

【0071】そして、この復号化したリクエストR（Kcs）をクライアントの公開鍵Kcpで復号化することにより送信要求に係わるクライアント側の電子署名の照合を行う（ステップ207）。

【0072】このステップ207の電子署名照合の結果、この電子署名が適正でないと判断した場合は（ステップ207でNO）、この送信要求を無視する（ステップ208）。

【0073】また、このステップ207の電子署名照合の結果、この電子署名が適正であると判断した場合は（ステップ207でOK）、次に、この送信要求が予約処理かを調べる（ステップ209）。ここで、予約処理でないと判断した場合は（ステップ209でNO）、送信要求の拒否通知Tを生成し（ステップ212）、ステップ213に移行する。

【0074】また、ステップ209において、この送信要求が予約処理であると判断した場合は（ステップ209でOK）、この送信要求に対応する電子データ T' （ $=R(Kcs) + \alpha$ ）を生成し（ステップ210）、次に、この電子データ T' に暗号化した通し番号を付与して（ステップ211）、電子データ $T (=T' + \text{通し番号})$ を生成し、ステップ213に移行する。

【0075】ステップ213では、電子データまたは拒否通知Tをサーバの秘密鍵Kssで暗号化することにより電子署名を行い、この電子署名した情報T（Kss）を更にクライアントの公開鍵Kcpで暗号化し（ステップ214）、この暗号化した情報T（Kss、Kcp）をクライアント側に送信する（ステップ215）。

【0076】クライアント側では、この情報T (K s s、K c p)を受信し(ステップ216)、この受信した情報T (K s s、K c p)をクライアントの秘密鍵K c sで復号化する(ステップ217)。

【0077】そして、この復号化した情報T (K s s)をサーバの公開鍵K s pで復号化することによりサーバ側の電子署名の照合を行う(ステップ218)。

【0078】このステップ218の電子署名照合の結果、この電子署名が適正でないと判断した場合は(ステップ218でNO)、この情報を無視する(ステップ219)。

【0079】また、このステップ218の電子署名照合の結果、この電子署名が適正であると判断した場合は(ステップ218でOK)、次に、この情報Tから送信要求の結果確認を行う(ステップ220)。

【0080】この結果確認により、情報Tが拒否通知である場合は(ステップ220でNO)、所定の予約エラー処理を実行する(ステップ221)。

【0081】また、この結果確認により、情報Tが送信要求に対応する電子データである場合は(ステップ220でOK)、記録装置に記録する(ステップ222)とともに、電子データT (K s s)の格納を行う(ステップ223)。

【0082】なお、ステップ218~222の処理を行うことなく、ステップ217から直接ステップ223に移行するように構成してもよい。

【0083】図7は、図1に示した電子データ送信システムにおける電子データ予約手順の他の具体例を示したもので、この図7の示すものにおいては、乱数を用いた場合におけるクライアント側のクライアント端末20およびサーバ側のサーバ端末10の動作を示している。

【0084】図7において、クライアント側からサーバ側に対して送信要求をする場合は、まず、この送信要求に対応するリクエストR'を生成する(ステップ301)。

【0085】そして、このリクエストR'に乱数を付与する(ステップ302)。その後、この乱数が付与されたリクエストR (R' + 乱数)をクライアントの秘密鍵K c sで暗号化することにより電子署名を行う(ステップ303)。

【0086】次に、この電子署名を行ったリクエストR (K c s)を更にサーバの公開鍵K s pで暗号化し(ステップ304)、この暗号化したリクエストR (K c s、K s p)をサーバ側に送信する(ステップ305)。

【0087】サーバ側では、このリクエストR (K c s、K s p)を受信し(ステップ306)、この受信したリクエストR (K c s、K s p)をサーバの秘密鍵K s sで復号化する(ステップ307)。

【0088】そして、この復号化したリクエストR (K

c s)をクライアントの公開鍵K c pで復号化することにより送信要求に係わるクライアント側の電子署名の照合を行う(ステップ308)。

【0089】このステップ308の電子署名照合の結果、この電子署名が適正でないと判断した場合は(ステップ308でNO)、この送信要求を無視する(ステップ309)。

【0090】また、このステップ308の電子署名照合の結果、この電子署名が適正であると判断した場合は(ステップ308でOK)、次に、この送信要求が予約処理かを調べる(ステップ310)。ここで、予約処理でないと判断した場合は(ステップ310でNO)、送信要求の拒否通知Tを生成し(ステップ312)、ステップ313に移行する。

【0091】また、ステップ310において、この送信要求が予約処理であると判断した場合は(ステップ310でOK)、この送信要求に対応する電子データT (= R (K c s) + α)を生成し(ステップ311)、ステップ313に移行する。

【0092】ステップ313では、電子データまたは拒否通知Tをサーバの秘密鍵K s sで暗号化することにより電子署名を行い、この電子署名した情報T (K s s)を更にクライアントの公開鍵K c pで暗号化し(ステップ314)、この暗号化した情報T (K s s、K c p)をクライアント側に送信する(ステップ315)。

【0093】クライアント側では、この情報T (K s s、K c p)を受信し(ステップ316)、この受信した情報T (K s s、K c p)をクライアントの秘密鍵K c sで復号化する(ステップ317)。

【0094】そして、この復号化した情報T (K s s)をサーバの公開鍵K s pで復号化することによりサーバ側の電子署名の照合を行う(ステップ318)。

【0095】このステップ318の電子署名照合の結果、この電子署名が適正でないと判断した場合は(ステップ318でNO)、この情報を無視する(ステップ319)。

【0096】また、このステップ318の電子署名照合の結果、この電子署名が適正であると判断した場合は(ステップ318でOK)、次に、この情報Tから送信要求の結果確認を行う(ステップ320)。

【0097】この結果確認により、情報Tが拒否通知である場合は(ステップ320でNO)、所定の予約エラー処理を実行する(ステップ321)。

【0098】また、この結果確認により、情報Tが送信要求に対応する電子データである場合は(ステップ320でOK)、記録装置に記録する(ステップ322)とともに、電子データT (K s s)の格納を行う(ステップ323)。

【0099】なお、ステップ318~322の処理を行うことなく、ステップ317から直接ステップ323に

移行するように構成してもよい。

【0100】図8は、図1に示した電子データ送信システムにおける電子データ利用手順の具体例を示したもので、図8においてはクライアント側のクライアント端末20および電子データ確認用端末側のチェック端末30の動作を示している。

【0101】なお、この実施例においてはクライアント側および電子データ確認用端末側における電子署名および暗号化／復号化処理のために、クライアント側のクライアント端末20は、秘密鍵Kcsおよび公開鍵Kcpを有しており、また、電子データ確認用端末側のチェック端末30は、秘密鍵Ktsおよび公開鍵Ktpを有している。

【0102】図8において、クライアント側ではサーバ側で電子署名された電子データT(Kss)が格納されている(ステップ401)。まず、クライアント側では、格納されているチケット、すなわち、電子データT(Kss)を取り出し(ステップ402)、この電子データT(Kss)を確認用端末の公開鍵Ktpで暗号化し(ステップ304)、この暗号化した電子データT(Kss、Ktp)を電子データ確認用端末側に送信する(ステップ404)。

【0103】電子データ確認用端末側では、この電子データT(Kss、Ktp)を受信し(ステップ405)、この受信した電子データT(Kss、Ktp)を確認用端末の秘密鍵Ktsで復号化する(ステップ406)。

【0104】そして、この復号化した電子データT(Kss)をサーバの公開鍵Kspで復号化することにより電子署名の照合を行う(ステップ407)。

【0105】このステップ407の電子署名照合の結果、この電子署名が適正でないと判断した場合は(ステップ407でNO)、この電子データT(Kss)を無視する(ステップ408)。

【0106】また、このステップ407の電子署名照合の結果、この電子署名が適正であると判断した場合は(ステップ407でOK)、次に、電子データT(Kss)の内容確認を行う(ステップ409)。

【0107】この内容確認の結果、電子データT(Kss)が適正でない場合は(ステップ409でNO)、所定のエラー処理を行う(ステップ410)。

【0108】また、この内容確認の結果、電子データT(Kss)が適正ある場合は(ステップ409でOK)、次に、電子データT(Kss)に付与されている暗号化された通し番号に重複があるか否かの番号重複確認を行う(ステップ411)。

【0109】ここで、通し番号に重複ありと判断された場合は、エラーとして所定のエラー処理を行う(ステップ412)。

【0110】また、ステップ411で通し番号に重複な

しと判断された場合は、電子データT(Kss)に対応する所定のチケット内容実行を行う(ステップ413)。

【0111】

【発明の効果】以上説明したように、この発明の電子データ送受信システムによれば、サーバは、電子データ送信手段により、クライアントからの送信要求に対応して暗号化した通し番号を付与した電子データをクライアントに送信するとともに、電子データ記憶手段により、電子データ送信手段で送信した電子データを記憶し、また、クライアントは、電子データ受信手段により、電子データ送信手段によりサーバから送信された電子データを受信することにより電子データの受信を行い、また、電子データ確認端末は、電子データ確認手段により、電子データ受信手段で受信した電子データと上記電子データ記憶手段に記憶した電子データとを照合することにより電子データの確認を行うように構成したので、送信された電子データの不正利用を防止するとともに、チケット送信の秘密の保持性に優れた電子データ送受信システムを提供することができるという効果を奏する。

【図面の簡単な説明】

【図1】この発明に係わる電子データ送受信システムの一実施例の概略構成を示すブロック図。

【図2】図1に示したサーバ端末の具体的構成を示すブロック図。

【図3】図2に示した基本ブロックの詳細構成を示すブロック図。

【図4】図1に示したクライアント端末の具体的構成を示すブロック図。

【図5】図1に示したチェッカ端末の具体的構成を示すブロック図。

【図6】図1に示した電子データ送信システムにおける電子データ予約手順の具体例を示したフローチャート。

【図7】図1に示した電子データ送信システムにおける電子データ予約手順の他の具体例を示したフローチャート。

【図8】図1に示した電子データ送信システムにおける電子データ利用手順の具体例を示したフローチャート。

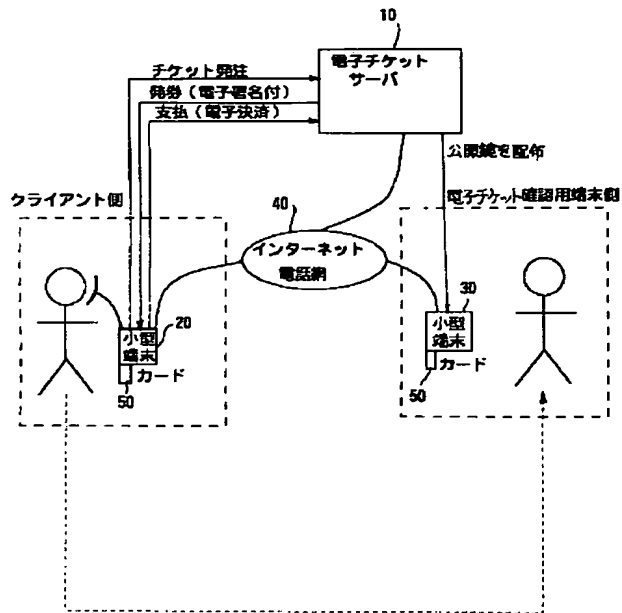
【符号の説明】

- 10 電子データサーバ(サーバ端末)
- 12 データベース
- 20 小型端末(クライアント端末)
- 21 入力装置
- 22 記憶域
- 23 表示装置
- 24 記録装置
- 25 電子決済装置
- 30 小型端末(チェッカ端末)
- 31 確認装置
- 32 表示装置

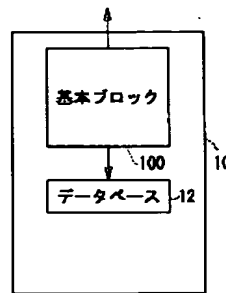
- 21
- 40 インタネット電話網
- 50 電子チケットカード (カード)
- 100 基本ブロック
- 101 識別子発生装置
- 102 時計
- 103 電源
- 104 通信部
- 105 作業域

- 22
- 110 暗号処理装置
- 111 電子署名装置
- 112 電子署名参照装置
- 113 暗号化装置
- 114 復号化装置
- 120 鍵管理装置
- 121 公開鍵管理装置
- 122 秘密鍵管理装置

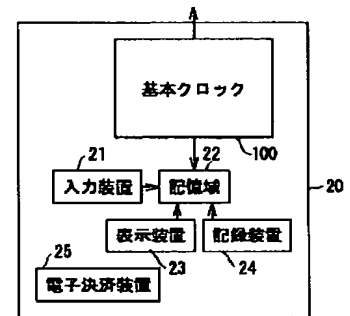
【図 1】



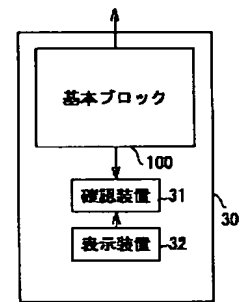
【図 2】



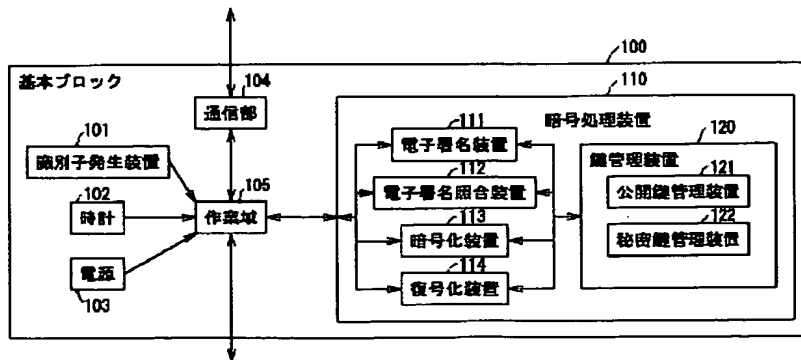
【図 4】



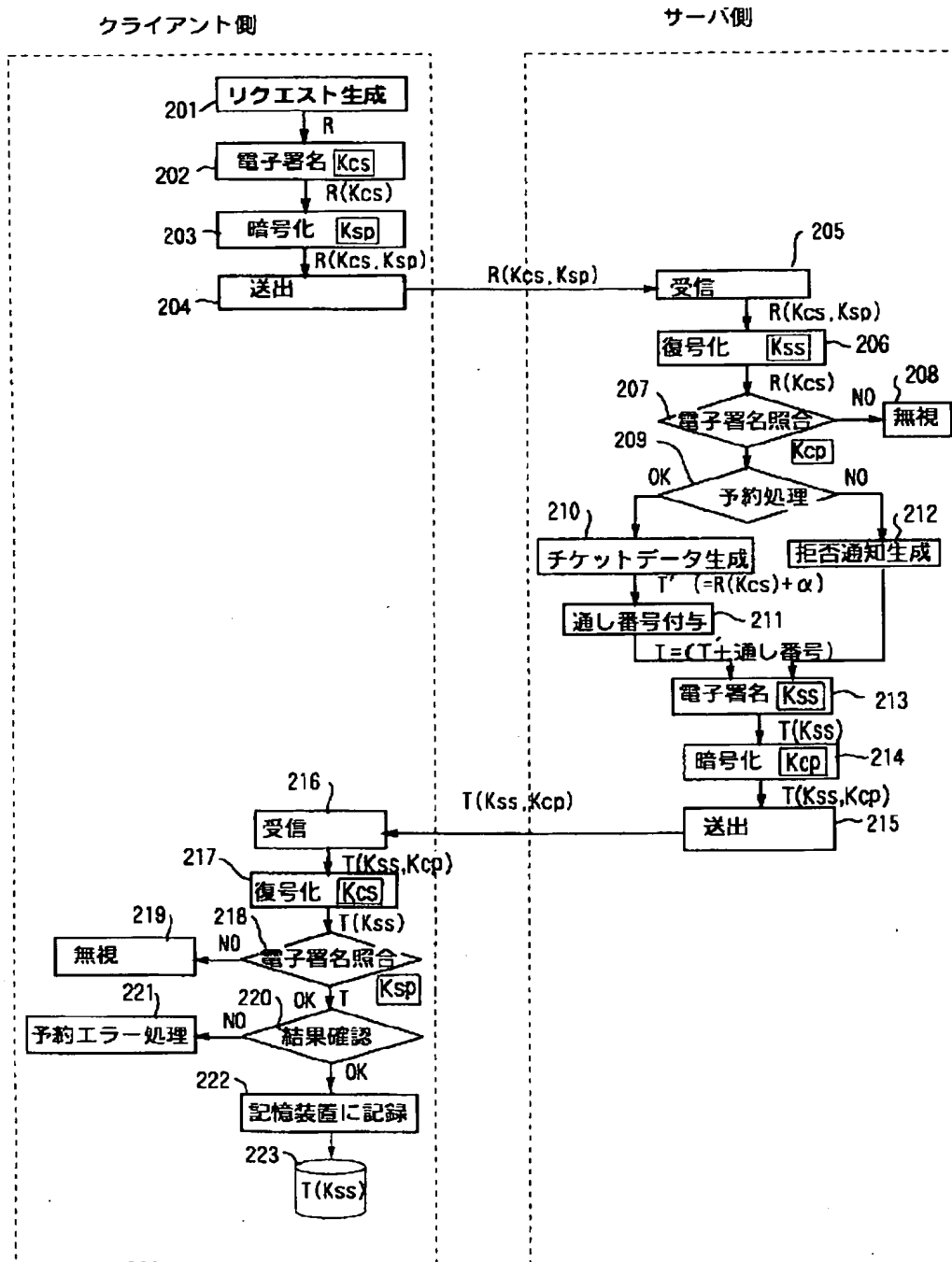
【図 5】



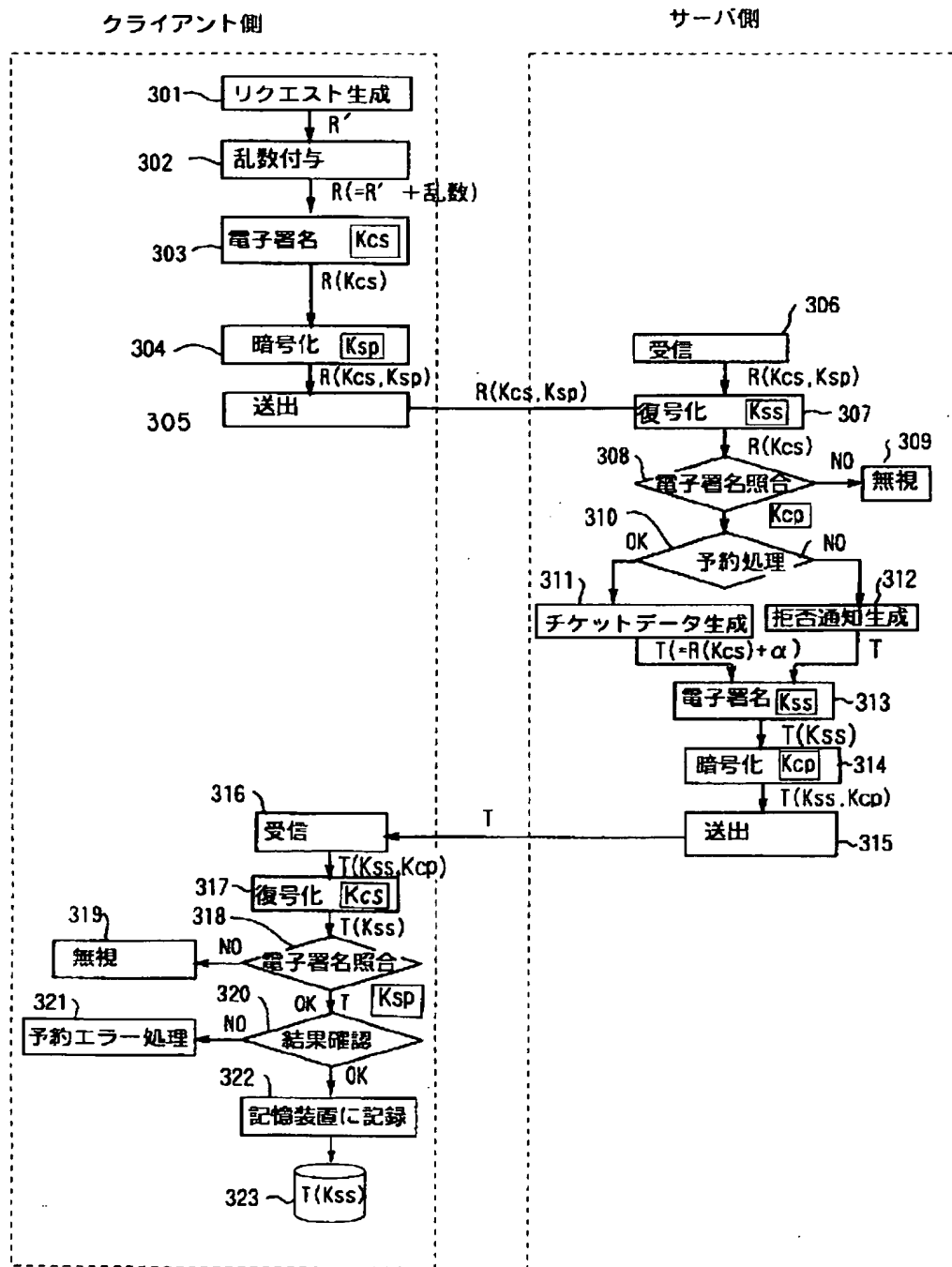
【図 3】



【図 6】



【図 7】



【図 8】

